Compression of IPsec AH and ESP Headers for Constrained Environments

draft-raza-6lo-ipsec-02

{shahid.raza, simon.duquennoy}@sics.se
goran.selandaer@ericsson.com

Status of the Document

- First submitted as a position paper to the Smart Object Workshop [RFC6574] co-located with IETF 80.
- Later submitted to 6LoWPAN WG
- Moved to 6lo and included in the 6lo BoF
- Presented in 6lo during the IETF93

Salient Features

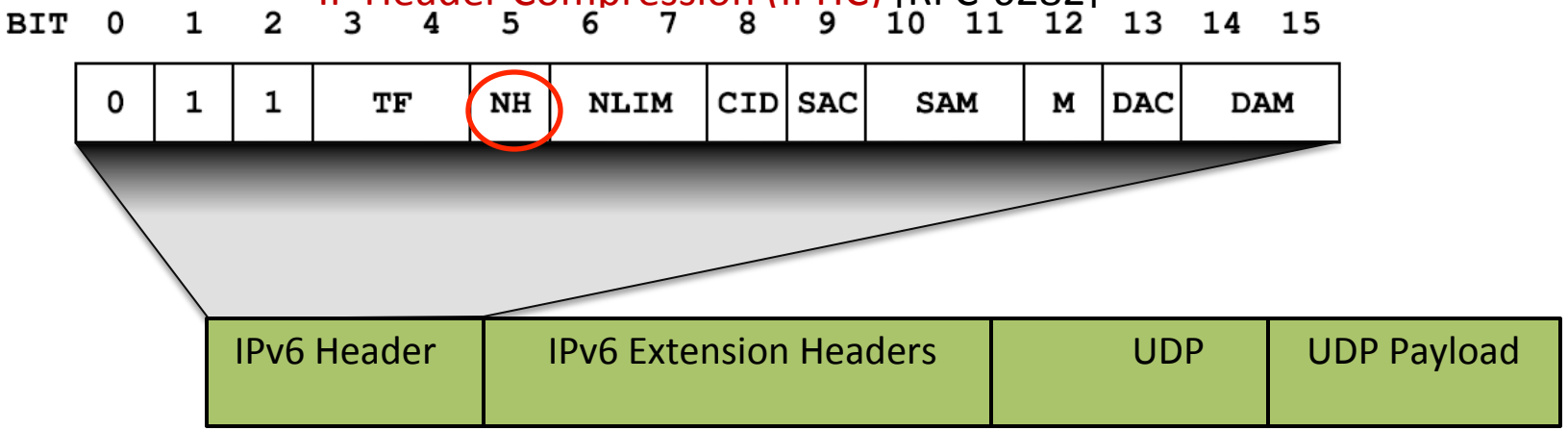
- Does not require any modification in the IPsec standard
  - End-to-End compatible with any IPsec enabled hosted on the Internet.
  - Only performs header compression within 6LoWPAN networks without compromising any security properties
- Seamlessly links with the 6LoWPAN standard
- Other compression mechanisms exists
  - draft-mglt-6lo-diet-esp-01 requires changes in the IPsec standard and should also be supported/enabled in hosts on the Internet
  - ROHC [RFC5795][RFC5856]) also targets any Internet hosts and not specific to 6LoWPAN networks
  - Both are complementary to our solution

IP Security (IPsec)

- End-to-end Security at the Network layer
  - Part of the OS
  - Protects IP and UDP/TCP headers
  - IPsec Transport mode for the Internet of Things
- Authentication Header (AH) [RFC-4302]
  - Integrity and authentication
- Encapsulated Security Payload (ESP) [RFC-4303]
  - Confidentiality and optionally integrity and authentication
- AH and ESP are *IP extension headers*
- IPv6 nodes SHOULD implement IPsec [RFC 6434]

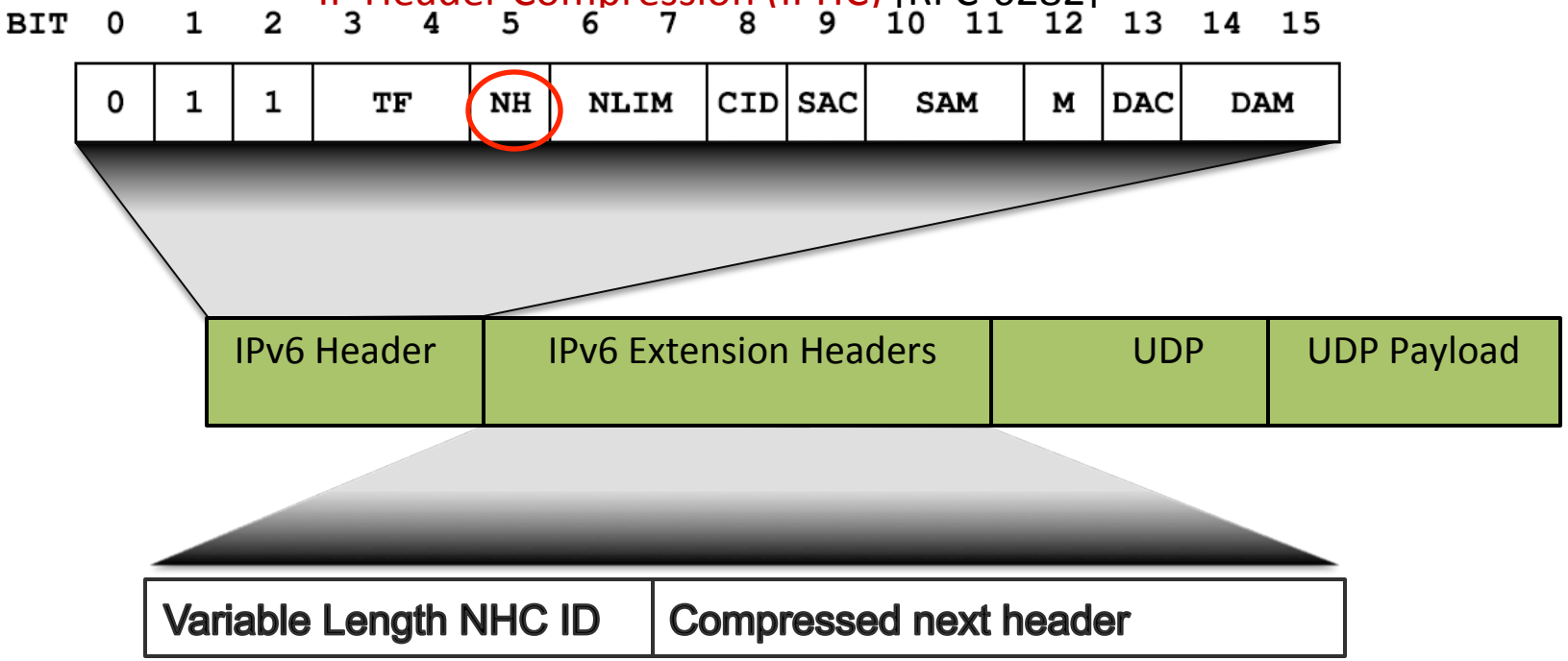
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]



Linking IPsec Headers Compression with 6LoWPAN

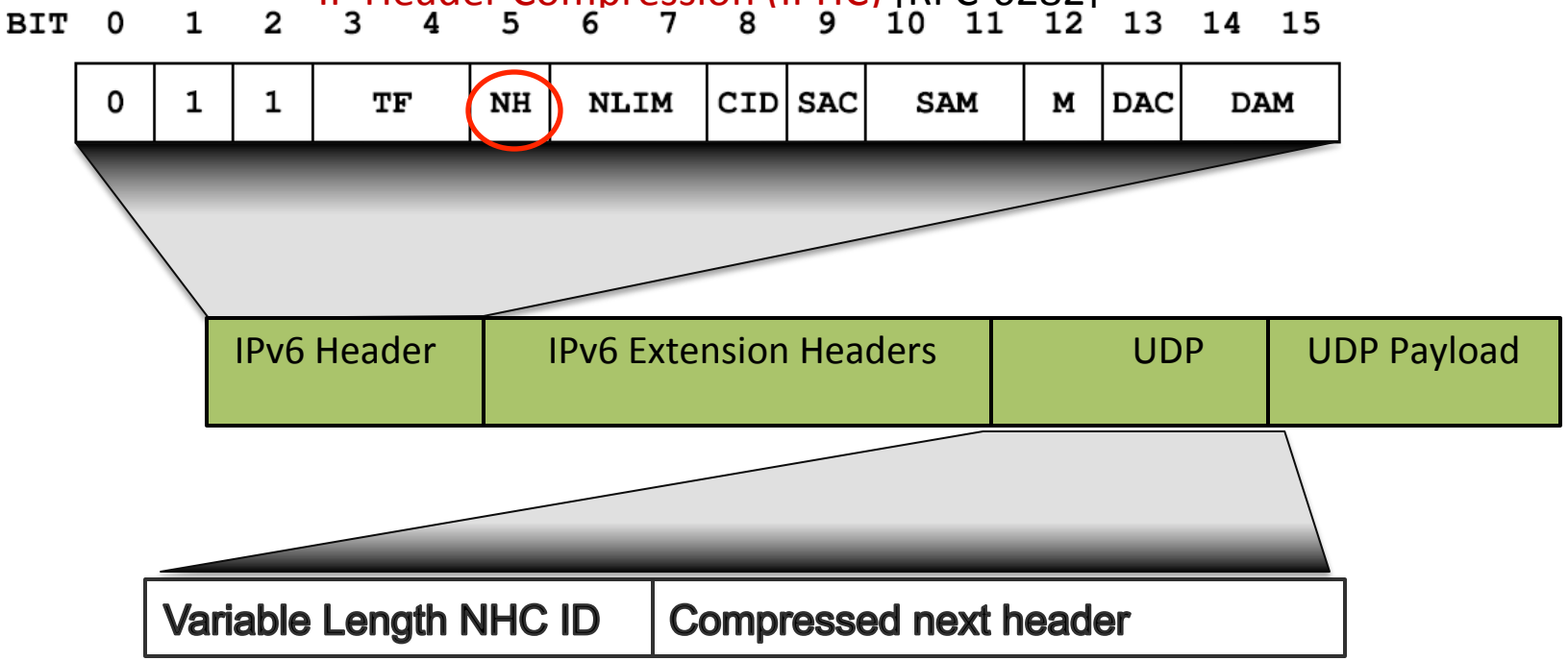
IP Header Compression (IPHC) [RFC-6282]



Next Header Compression (NHC) [RFC-6282]

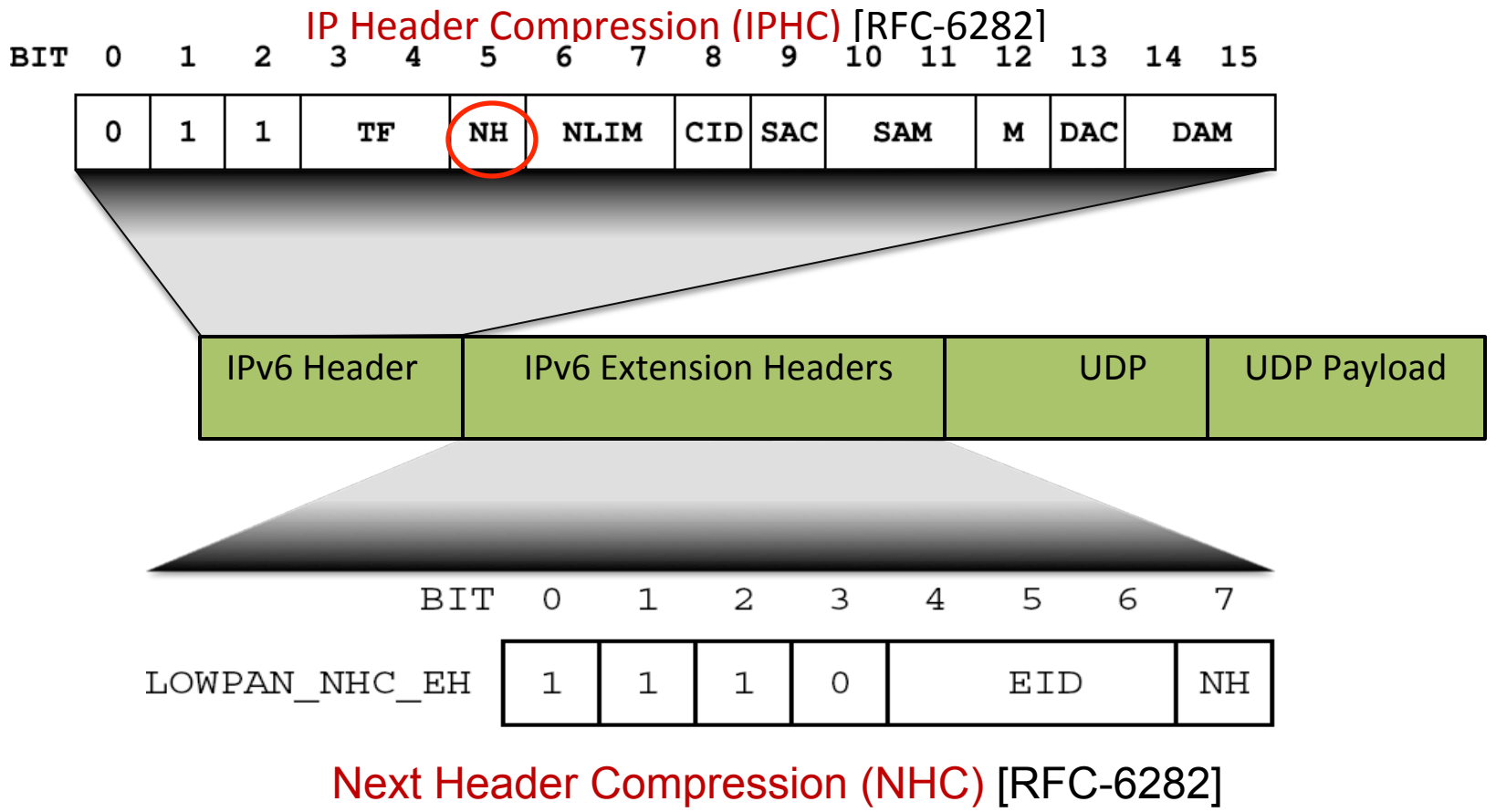
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]

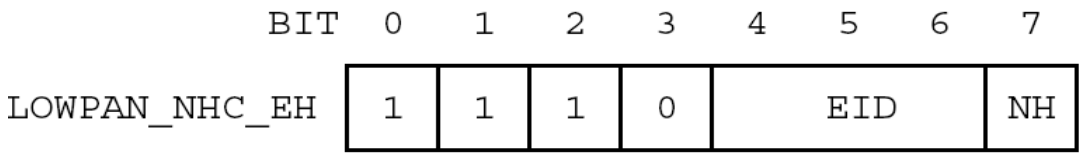


Next Header Compression (NHC) [RFC-6282]

Linking IPsec Headers Compression with 6LoWPAN



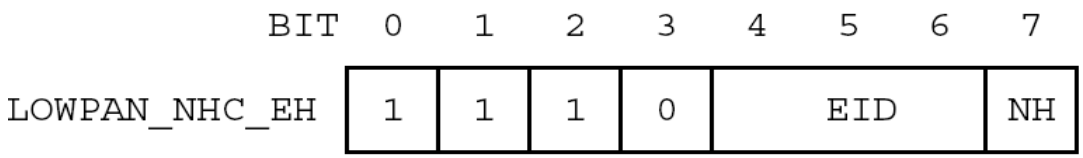
Linking IPsec Headers Compression with 6LoWPAN (cont…)



Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved -
6: Reserved -
7: IPv6 Header

Linking IPsec Headers Compression with 6LoWPAN (cont…)

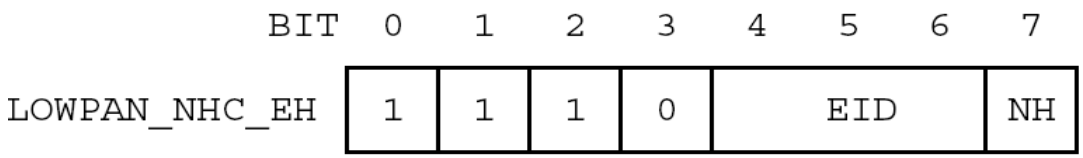


Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved -
6: Reserved -
7: IPv6 Header

Extension Header Order [RFC2460]
IPv6 header
Hop-by-Hop Options header
Destination Options header
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header
upper-layer header

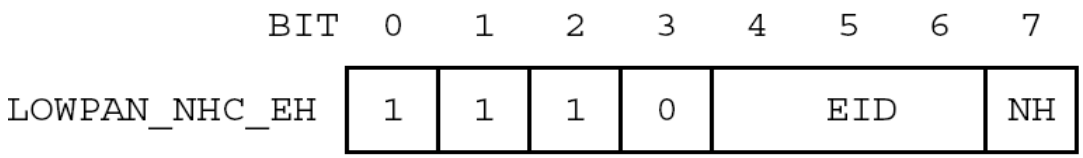
Linking IPsec Headers Compression with 6LoWPAN (cont…)



Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved - IPv6 Authentication Header
6: Reserved -IPv6 Encapsulated Security Payload
7: IPv6 Header

Linking IPsec Headers Compression with 6LoWPAN (cont…)



Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved - IPv6 Authentication Header
6: Reserved -IPv6 Encapsulated Security Payload
7: IPv6 Header

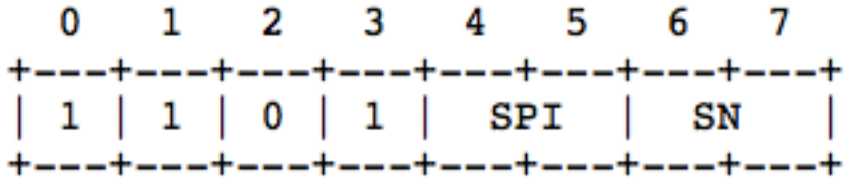
Proposal 2 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved
6: *Reserved IPv6 Authentication Header & IPv6 Encapsulated Security Payload
7: IPv6 Header

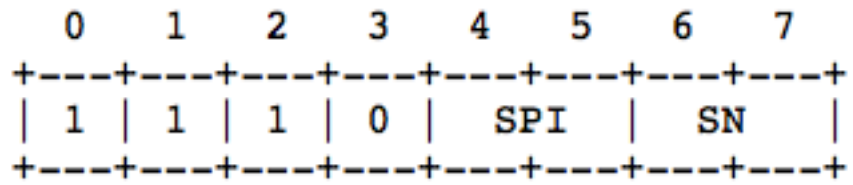
**** Variable length NHC ID is used to distinguish AH and ESP***

Compressing IPsec (cont...)

- Proposed LOWPAN NHC encoding for AH

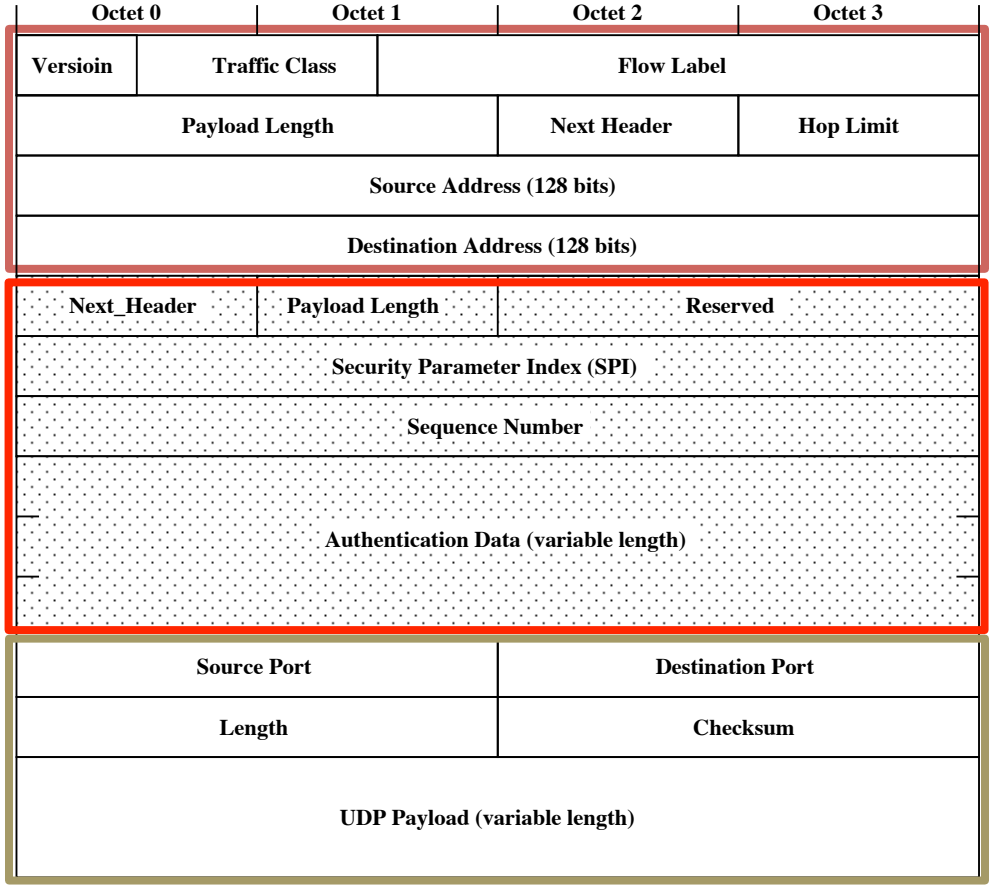


- Proposed LOWPAN NHC encoding for ESP

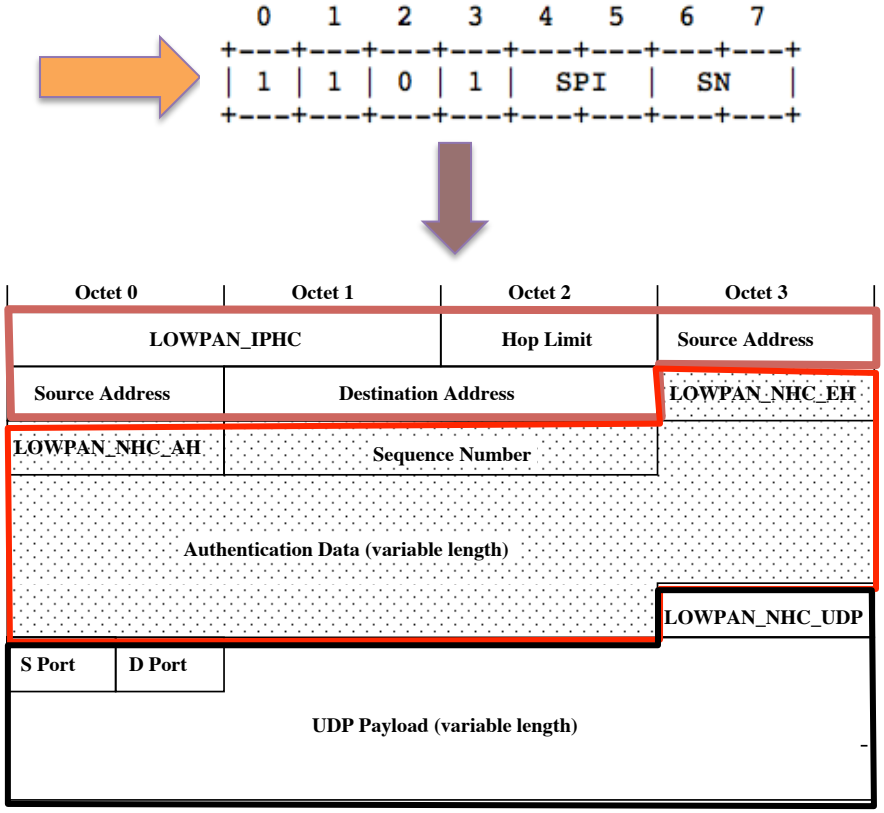


- SPI: Security Parameter Index
- SN: Sequence Number

Compressed IPsec AH



IP Datagram secured with AH



Compressed IP Datagram secured with compressed AH

Compressed IPsec AH
(Packet Size comparison)

Service	Without IPsec Compression [Byte]	With IPsec Compression [Byte]
Integrity with AH [HMAC-SHA1-96]	12*	4*
Confidentiality with ESP [AES-CTR]	10**	4**
Confidentiality and Integrity with ESP [AES-CTR] and [HMAC-SHA1-96]	10***	4***

* *Plus 12 bytes of Authentication data*
** *Plus 8 bytes of Initialization Vector*
*** *Plus 12 bytes of Authentication data and 8 bytes of Initialization Vector*

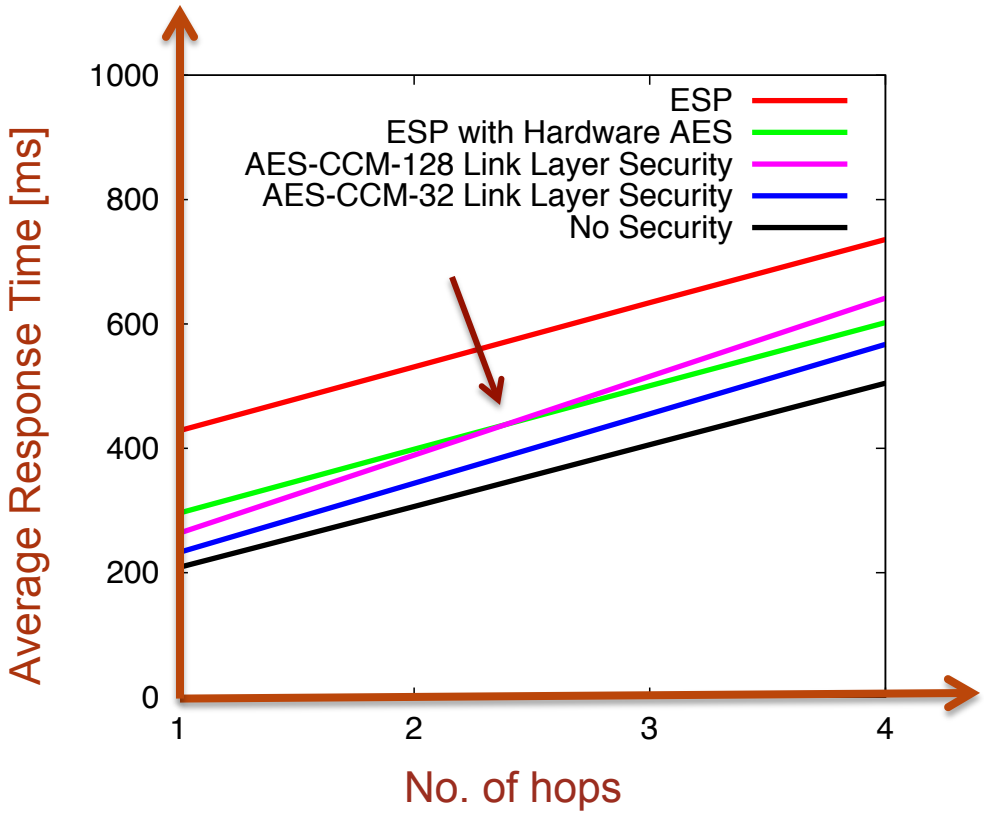
Compressed IPsec
(Implementation)

- We implement IPSec in Contiki OS
  - uIPv6 with AH and ESP
  - SICSLoWPAN with AH and ESP
  - Set of standardized cryptographic algorithms
- Even suitable for Class 0 devices [RFC7228]

System	ROM (kB)		RAM (kB)	
	overall	diff	overall	diff
Without IPsec	32.9	–	8.0	–
AH with HMAC-SHA1-96	36.8	3.9	9.1	1.1
AH with XCBC-MAC-96	38.4	5.5	8.5	0.5
ESP with AES-CBC	41.4	8.5	8.3	0.3
ESP with AES-CTR	39.8	6.9	9.1	0.3
ESP with AES-XCBC-MAC-96	39.8	6.9	8.3	0.3
ESP with AES-CBC + AES-XCBC-MAC-96	41.9	9.0	8.3	0.3
ESP with AES-CBC + AES-XCBC-MAC-96	41.9	9.0	8.3	0.3

IPsec vs. IEEE 802.15.4 security

- Multi hops with 512 byte data size



Shahid Raza, et al., *Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN.* **Journal of Security and Communication Networks, 7(12), December 2014**

Questions/Comments

shahid@sics.se

Source Code

svn co https://contikiprojects.svn.sourceforge.net/svnroot/contikiprojects/sics.se/ipsec ipsec